(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 May 2004 (21.05.2004)

PCT

(10) International Publication Number
WO 2004/043098 A1

(51) International Patent Classification[7]: H04Q 7/38, 7/32

(21) International Application Number:
PCT/CA2003/000955

(22) International Filing Date: 23 June 2003 (23.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/423,355 4 November 2002 (04.11.2002) US

(71) Applicant (*for all designated States except US*): **RESEARCH IN MOTION LIMITED** [CA/CA]; 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): **ISLAM, Khaledul** [CA/CA]; 88 Broughton Street, Kanata, Ontario K2K 3N4 (CA). **HOSSAIN, Asif** [BD/CA]; 163 Flamborough Way, Kanata, Ontario K2K 3H9 (CA).

(74) Agents: **PATHIYAL, Krishna, K.** et al.; Research In Motion Limited, 295 Phillip Street, Waterloo, Ontario N2L 3W8 (CA).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

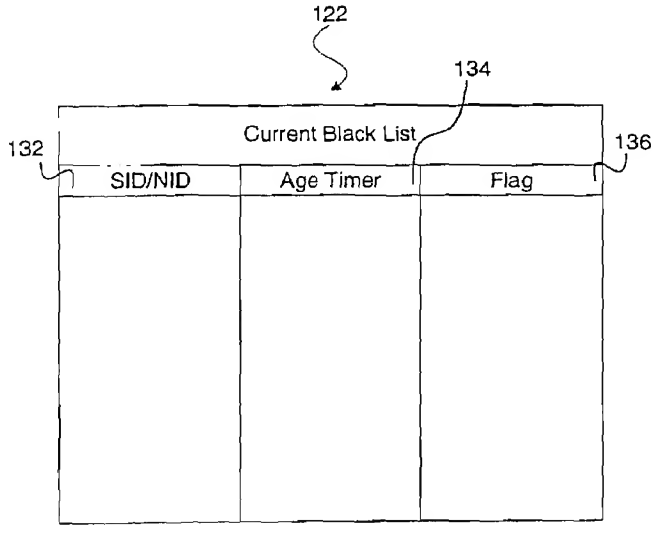
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR PACKET DATA SERVICE DISCOVERY



(57) Abstract: A method and apparatus for packet data service discovery are described. A current blacklist comprising entries for wireless networks not providing packet data services (i.e. either not supporting the services or not having a packet data services roaming agreement) is kept in memory of the mobile device based on previous attempts to connect to such networks. Current preferred roaming lists identify whether a given wireless network can be acquired, but do not identify whether a data services roaming agreement exists. At least one of the following advantages is provided: no advance knowledge of data services roaming agreements is required; no mobile device software change is required when the data services roaming agreement changes; mobile device can notify a server of a wireless network status change; significant power savings at the mobile device; and avoid unnecessary network access, which in turn saves network resources and capacity.

WO 2004/043098 A1

MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD AND APPARATUS FOR PACKET DATA SERVICE DISCOVERY

[0001] This application claims the benefit of priority from United States Provisional Patent Application Serial No. 60/423355 filed on November 4, 2002.

FIELD OF THE INVENTION

[0002] The present invention relates to the discovery of services provided for a mobile device in a wireless network without any a priori knowledge. The invention relates particularly to the discovery of packet data services provided for mobile devices.

BACKGROUND OF THE INVENTION

[0003] In a CDMA (Code Division Multiple Access) network, a system identifier (SID) identifies a service provider as well as a given geographical area. Networks within a system are given a network identifier or NID. A network is uniquely identified by the pair (SID, NID). **Fig. 1** illustrates a network cloud **100** showing the relationship between various system identifiers and network identifiers.

[0004] A CDMA mobile device is typically pre-programmed by operators with an entity called a Preferred Roaming List (PRL). A PRL can also be downloaded to the mobile device using known over the air provisioning methods. **Fig. 2** illustrates a simplified representation of a conventional preferred roaming list **102**. The PRL, which comprises of a number of records, indicates which systems the mobile device is allowed to acquire. In this example, each record identifies a system by its (SID, NID) pair and provides the frequencies that the mobile device is to use when attempting to acquire the system. For each record, there can be an indicator of whether the system is preferred, the roaming status, the relative priority of the system, and its geographic region. As part of system acquisition, the mobile device searches for a CDMA Pilot Channel on a set of frequencies based on the PRL. The (SID/NID) information of the acquired system is conveyed to the mobile device on a Sync Channel once the mobile device has acquired the Pilot Channel. The PRL only contains the information about which systems the mobile device is allowed to acquire. It does not have any information about the type of services that are allowed on a given network. Typically, it only indicates that a certain degree of voice service is available on a network.

[0005] An "always-on always connected" mobile device needs to maintain data connectivity all the time to support seamless mobility. This requires the mobile device to re-establish its data connectivity whenever it changes systems. However, the mobile device has no a priori knowledge as to whether it is allowed to make a data call on a given system. Even if the network indicates that it is capable of supporting packet data services, there is no guarantee that the mobile device will be allowed to make any data calls. The mobile device can only find out about such information after it makes a data call origination attempt. A mobile device can only have true data mobility if a data roaming services agreement exists between the relevant service providers. A roaming agreement between operators does not necessarily cover all available services. For example, two operators may have a voice services roaming agreement, but no packet data services roaming agreement. Currently, there is no standardized mechanism to convey this information to the mobile device. As a result, the mobile device is forced to make blind data call origination attempts to find out whether it is allowed to make data calls or not. This has a significant impact on the battery life, especially in a geographical area where the mobile device goes in and out of a system where data calls are not allowed. Therefore, there is a need for a device capable of efficiently handling interactions with a network with respect to data service availability.

SUMMARY OF THE INVENTION

[0006] It is an object of the present invention to obviate or mitigate at least one disadvantage of previous service discovery arrangements. It is particularly advantageous to provide an improvement with respect to the discovery of data services for mobile devices.

[0007] According to an aspect of the invention, there is provided a mobile device capable of supporting packet data services offered by wireless networks. The mobile device includes a memory, as well as a transceiver for exchanging packet data service authentication information with the wireless networks. The mobile device also includes a current blacklist provided in the memory, the current blacklist identifying wireless networks that do not provide packet data services to the mobile device, the current blacklist being based on previous packet data service authentication rejections. The mobile device further includes a processor for updating the current blacklist in response to newly received packet data service authentication information.

[0008] According to another aspect of the invention, there is provided a method of data service discovery for a mobile device having a current blacklist. The method includes the following steps: detecting a wireless network; examining the current blacklist stored on the mobile device; if the detected wireless network is listed in the current blacklist, refraining from making any packet data call attempts for a predetermined period of time. Otherwise, the method includes the following steps: determining whether the wireless network provides packet data services to the mobile device, and adding the wireless network to the current blacklist if the wireless network does not provide packet data services to the mobile device.

[0009] According to a further aspect of the invention, there is provided a method of packet data service notification in a wireless network, the wireless network including a server and a mobile device. The method includes the following steps: receiving at the server a registration of a newly powered-up mobile device; retrieving a server-stored current blacklist identifying wireless networks that do not provide packet data services to the newly powered-up mobile device; and sending the server-stored current blacklist from the server to the newly powered-up mobile device for reception by and storage on the mobile device.

[0010] Other aspects and features of the present invention will become apparent to those ordinarily skilled in the art upon review of the following description of specific embodiments of the invention in conjunction with the accompanying figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] Embodiments of the present invention will now be described, by way of example only, with reference to the attached figures, wherein:

Fig. 1 illustrates a network cloud showing the relationship between various system identifiers and network identifiers;

Fig. 2 illustrates a simplified representation of a conventional preferred roaming list;

Fig. 3 illustrates a system used for authentication in a simple IP network;

Fig. 4 illustrates a system used for authentication in a mobile IP network;

Fig. 5 illustrates a mobile device according to an embodiment of the present invention in the context of wireless network components and a home server of the mobile device;

Fig. 6A and **Fig. 6B** illustrate a flowchart showing steps in a method according to an embodiment of the present invention;

Fig. 7 illustrates a representation of an exemplary current blacklist according to an embodiment of the present invention; and

Fig. 8 illustrates the relationship between a conventional OSI network layer model and a layer model for a mobile device.

DETAILED DESCRIPTION

[0012] Generally, the present invention provides a method and apparatus for packet data service discovery without any a priori knowledge. A current blacklist comprising entries for wireless networks not providing packet data services is kept in a mobile device's memory, in order to avoid unnecessary repeated requests to such networks. Current preferred roaming lists can identify whether a given wireless network can be acquired, but do not identify whether a data services roaming agreement exists. A mobile device, or mobile station, according to the invention, or employing a method according to the invention, dynamically "auto-discovers" the wireless networks on which it is permitted to make packet data calls. A list of wireless networks not providing packet data services (i.e. either not supporting the services or not having a packet data services roaming agreement) is kept in memory of the mobile device based on previous attempts to connect to such networks.

[0013] The present invention provides at least one of the following advantages: no advance knowledge of data roaming agreements is required at the mobile device; no mobile device software change is required when a data roaming agreement changes; the mobile device can notify its home server regarding a change of status of any wireless network; significant power savings are realized at the mobile device; and unnecessary wireless network access is avoided in a network, which saves network resources and capacity.

[0014] The following paragraphs provide definitions for terms that will be used in the specification.

[0015] The term "mobile device" as used herein includes any electronic device having at least voice and data communication capabilities. The mobile device is preferably a two-way wireless communication device capable of supporting both voice services and packet data services. Although reference is made in the description to the use

and provision of packet data services, the invention can advantageously be used with other types of data services. Depending on the exact functionality provided, the mobile device may be referred to in the art by different terms, for example, as a data messaging device, a two-way pager, a wireless e-mail device, a cellular telephone with data messaging capabilities, a wireless Internet appliance, or a data communication device.

[0016] The term "wireless network" as used herein includes any network or system, or the operator or carrier of such a network or system, having at least one component that provides wireless or mobile services, for example packet data services, to a mobile device.

[0017] A wireless network that "supports" packet data services has the necessary hardware and software in place to be capable of offering packet data services to a mobile device. A wireless network that "does not support" packet data services does not have the necessary hardware and software in place to be capable of offering packet data services to a mobile device.

[0018] A wireless network "provides" packet data services to a mobile device when it supports packet data services and also permits, or allows, that mobile device to use the packet data services. This permission can be, for example, pursuant to a packet data services roaming agreement between carriers, service providers, or network operators. A wireless network that "does not provide" packet data services to a mobile device either does not support packet data services, or it supports packet data services, but the mobile device is not permitted to use the packet data services, for example due to a lack of a packet data services roaming agreement.

[0019] There are two main types of CDMA packet data networks with which embodiments of the present invention can be used. The first type is a Simple IP (SIP) network in which a mobile device does not have a fixed Internet Protocol (IP) address. The IP address of a mobile device in a SIP network changes over time, with respect to location, etc. Once radio link protocol communication is established between the mobile device and a Radio Network (RN), the RN initiates an R-P interface between the RN and a Packet Data Serving Node (PDSN). The mobile device is authenticated by the serving PDSN via a RADIUS server and is subsequently assigned an IP address. The PDSN then provides the mobile device with connectivity, for instance to the Internet, an intranet (not shown), or generally an IP network. As the mobile device moves across PDSN boundaries, it is assigned new IP addresses, as necessary. An "always-on always

connected" mobile device typically notifies its home server of its own IP address so that packets can be pushed to it from its own server (e.g. an enterprise server). Typically, the Home Server IP address is fixed and known to the mobile device.

[0020] The second type is a Mobile IP (MIP) network in which a mobile device can have a static IP address, which is assigned by its home wireless network. The Home Agent IP address is also programmed into the mobile device. As the mobile device roams to a foreign network and attempts to set up a data session, the Foreign Agent (which is in effect a PDSN) communicates with the mobile device's specified Home Agent and then assigns the mobile device a Care-of Address (CoA). The home IP address of a mobile device in a MIP network can remain the same regardless of location, time, etc. Other devices or servers sending data to the mobile device only need to know about its home IP address, not the CoA.

[0021] Specific examples of SIP and MIP networks will be described in further detail in relation to **Fig. 3** and **Fig. 4**, respectively. **Fig. 3** illustrates a system used for authentication in a simple IP network.

[0022] In **Fig. 3**, a mobile device **104** communicates with a Radio Network (RN) **106**. The RN **106** performs functions such as call setup, handling handoff, performing tasks at a Radio Link Protocol (RLP) Layer and below. The RN **106** also communicates with a packet data serving node (PDSN) **108**. A PDSN, used in third generation (3G) networks, has a range of IP addresses and performs IP address management, maintains a session, and may perform caching. A PDSN provides access to the Internet, intranets and Wireless Application Protocol (WAP) servers for mobile devices utilizing a RN. It provides foreign agent (FA) support in MIP networks and packet transport for virtual private networking.

[0023] A Remote Authentication Dial-In User Service (RADIUS) server **110** is responsible for performing functions related to authentication, authorization, and accounting (AAA) of packet data services. It is also known as an AAA server. The RADIUS server **110** is connected to IP network **112**. The PDSN **108** communicates with other network entities, such as other RADIUS servers, via the IP network **112**.

[0024] The authentication steps in a SIP system such as in **Fig. 3**, generally comprise system access authentication and data authentication. The system access authentication is performed by a home location register/authentication center (HLR/AC) as a first level of authentication. In a system access authentication step, the RN **106** sends

a global challenge, and the mobile device **104** sends a response. This step is performed before the data session is established.

[0025] Next, a data authentication step is performed. This is typically done by means of known schemes such as Challenge-Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP).

[0026] If there is no data roaming agreement, one of the authentication steps (typically the data authentication step) will fail. Since there is no standard definition of what to do in such a case, the mobile device keeps trying. This is relevant to an "always-on, always connected" mobile device that is expected to maintain data connectivity at all times. Furthermore, according to the CDMA standard, a "dormant" mobile device is required to reconnect an existing dormant data connection every time there is a change in the NID, SID or packet zone identifier. A "dormant" mobile device has already established a PPP context with the network, but a reconnect attempt to a new wireless network can still fail. In addition, an "always-on, always connected" mobile device may be required to notify its Home Server if there is any change in the current SID in order to facilitate proper and efficient routing of data from the Home Server to the appropriate gateway. Repeated failed attempts to setup a data session in such conditions have the effect of unnecessarily increasing the amount of network traffic, and also reduce the battery life of the mobile device. In addition, if the mobile device is on the edge of a service area, there can be a "ping-pong" effect as the device alternates between trying to authenticate on a home network and on a foreign network.

[0027] **Fig. 4** illustrates a system used for authentication in a MIP network. In **Fig. 4**, the mobile device **104** stores a fixed home IP address, a fixed home agent address, and may store a fixed home server address. The PDSN **108** in **Fig. 4** can also be referred to as the foreign agent. The foreign agent **108** communicates with a home agent **114**, which has its own RADIUS server **116**. Once the foreign agent **108** finds out the necessary information to communicate with the home agent **114**, the authentication is actually performed at the home agent **114**. The home agent **114** receives all packets intended for the mobile device **104** and forwards them on to the foreign agent **108**, which in turn forwards them to the mobile device. The home agent **114** stores a CoA for the mobile device **104** and maps the home IP address of the mobile device to the CoA. In **Fig. 4**, the RN of the PDSN serving node can communicate via a mobile station controller (MSC) **118** to a home location register (HLR) **120** via SS7 network **122**.

[0028] The authentication steps in a MIP system include an initial system access authentication step, as is the case with SIP. However, in a MIP network, the subsequent data authentication step comprises a plurality of steps, such as: a foreign agent challenge (where the foreign agent sends a message asking the mobile device to respond); an MN-AAA_H authentication step; and an MN-HA authentication step, where MN represents a mobile node or mobile device, AAA_H represents a home RADIUS or AAA server, and HA represents a home agent. The data authentication step can comprise one or more of these levels of authentication. If any one of these authentication steps fails, this indicates that there is no data roaming agreement.

[0029] **Fig. 5** illustrates a mobile device according to an embodiment of the present invention in the context of wireless network components and a home server of the mobile device. The mobile device **104** communicates with the RN **106**, which in turn can communicate with the PDSN **108**, as described earlier. The PDSN **108** can communicate with a home server **128** associated with the mobile device by means of intermediary devices, such as illustrated in **Fig. 5** by Router A **124** on the PDSN side and Router B **126** on the home server side.

[0030] **Fig. 5** shows the mobile device having a current blacklist **122**. A blacklist as used herein represents a collection of data identifying wireless networks that do not provide packet data services to the mobile device. The blacklist is preferably stored in a form in which each listed network can be uniquely identified, and will be described in further detail below. Such a blacklist is in contrast to a preferred roaming list, which is known in the art, in which a listing of systems or networks allowing voice services is typically kept. Storing and using a blacklist helps to avoid unnecessary attempts to repeatedly access data services on the same wireless network. The current blacklist **122** identifies wireless networks that do not currently provide packet data services to the mobile device and is stored in memory on the mobile device. The current blacklist **122** is based on previous data relating to packet data service availability. Such data can be obtained as follows.

[0031] The mobile device **104** typically has a processor and transceiver, which includes a transmitter and a receiver. The receiver is used to decode information frames received over the air from the wireless network. The information frames can carry higher layer protocol stack payload and may contain payload from different entities in the wireless network, such as a PDSN. The received information frames are passed to the

processor, which then determines the next course of action. The transmitter is used to send over the air information frames to the wireless network as directed by the processor. The information frames carry payloads of higher layers in the protocol stack.

[0032] In terms of data authentication, the processor typically processes incoming packet data service authentication frames received from the wireless network, as well as outgoing packet data service authentication frames sent from the mobile device. The general steps relating to the exchange of such packet data service authentication frames is known in the art. For instance, an incoming packet data service authentication frame can contain a packet data service authentication request. In response to that request, the processor prepares the proper response. That response is sent by means of an outgoing packet data service authentication frame. The wireless network then performs authentication steps. Information relating to an authentication acceptance or rejection is typically sent to the mobile device. Of course, any of these exchanges can comprise, or be separated into, one or more information frames, packets or other unit of data transmission.

[0033] The exchange of packet data service authentication information between the mobile device and the wireless network is typically initiated in the context of the mobile device making a packet data call attempt on the wireless network. The authentication steps are simply a part of the data call process.

[0034] The current blacklist **122** is based on previous processed incoming packet data service authentication information. When packet data services are not provided to the mobile device, a packet data service authentication rejection is received from the wireless network. Therefore, the current blacklist is **122** is, in particular, based on received packet data service authentication rejections. The current blacklist **122** is also updated by the processor in response to newly received packet data service authentication rejections. The current blacklist **122** advantageously identifies a wireless network by its system identifier and network identifier pair, as will be described later in relation to **Fig. 7**.

[0035] In a particular embodiment, the current blacklist includes a timer value for each system that does not provide packet data services to the mobile device. The inclusion of a timer value is intended to provide an opportunity to send a subsequent packet data service authentication request at a suitable time, in order to determine if the situation has changed with respect to the wireless network not providing packet data services. The timer value can advantageously be implemented as an age timer, as is known to those skilled in the art. The selection of values to be used in the age timer **134** as shown in **Fig.**

7 can be based on knowledge of system parameters and the likelihood of change in such parameters. For instance, for a wireless network known to be having problems with or changes to its network equipment, the age timer can be set anywhere from a number of minutes to a number of days. For a wireless network which is the subject of negotiations to provide data roaming services, the age timer can be set anywhere from a number of days to a number of weeks or months, to monitor for any anticipated changes.

[0036] As described above, the mobile device maintains and updates its own current blacklist. This is advantageous since each mobile device can have its own particular abilities and requirements with respect to wireless networks it can acquire. The current blacklist is preferably stored in memory on the mobile device. In another embodiment, information stored in the mobile device's current blacklist can be transmitted to a server. The current blacklist can include a flag indicating whether an identification of a blacklisted wireless network has been passed to a server. Any portion of a current blacklist can advantageously be sent from the mobile device to a remote server, such as its home server, where the information can then be stored.

[0037] The server can gather current information relating to various wireless networks from a plurality of mobile devices. The server can send a server-stored current blacklist to a mobile device in particular instances where such transmission would be beneficial. For example, if a mobile device loses the information in its current blacklist, rather than building it from scratch, it could receive a server-stored current blacklist. The server-stored current blacklist can be stored in a memory of the particular server, or another server with which the server is in communications. The server can build a composite current blacklist based on reports from different mobile devices. This stored information can then be re-sent to other mobile stations.

[0038] **Fig. 6A** and **Fig. 6B** illustrate a flowchart showing steps in a method according to an embodiment of the present invention. In step **200**, in **Fig. 6A**, a mobile device starts acquisition of a system, or wireless network, based on the information in the PRL and the setting of network scan mode as specified by the user. The system acquisition can be initiated by any one of a number of situations, such as: turning the mobile device's radio functions on, change/loss of service; attempt to receive better service; network-directed redirection; rescan for a preferred system; etc.

[0039] Once a system has been acquired, it is preferably determined in step **202** whether the mobile device is required to send CDMA registration. If the system requires registration, a registration attempt is initiated. In step **204**, it is determined whether the CDMA registration attempt was successful. If yes, the method continues to step **206**; if not, the method returns to the first step **200** and attempts to acquire a different system. Steps **200-204** are steps that are used in known methods of data service discovery.

[0040] In step **206**, it is determined whether the acquired CDMA system, or network, supports or may support packet data services. The system will typically have an indicator to convey whether packet data services are supported. An example of such an indicator is the protocol revision of the RN, e.g. protocol revision greater than or equal to 6 in a CDMA2000 network.

[0041] However, such an indicator is not an absolute guarantee that packet data services are supported since a protocol revision of 6 (IS-2000 release 0) in such a network does not necessarily mean that packet data services are supported. Further steps in the method will confirm whether packet data services are provided, or permitted, with respect to the mobile device; this step simply rules out situations where such services are definitely not supported. If the network does not support packet data service (e.g. protocol revision < 6 in a CDMAOne network), then, referring to step **208**, the mobile device allows only voice and SMS traffic and notifies a user that packet data services are not available. If the network indicates that it supports or may support packet data services then the method proceeds to step **210**.

[0042] In step **210**, a determination is made as to whether the current system, or wireless network, is in a current blacklist. This is typically done by comparing the current SID with SID values stored in the current blacklist. If the current SID is found in the current blacklist, the method proceeds to step **212** in which the mobile device allows only voice and SMS traffic and notifies a user that packet data services are not provided by the current network. No data call attempt is made in such a case.

[0043] If the current SID is not in the current blacklist, the method proceeds to step **214** in **Fig. 6B** (if the mobile device does not already have an active data session). This is the case when the radio is turned ON or the mobile device cannot establish a data session on previously visited systems. In this step, the mobile device attempts to establish a data call. This can be achieved by the mobile device initiating a packet data call to setup a PPP session and attempting to get an IP address. If the mobile device has already established a

data session, i.e. it is in a dormant state with an IP address, the method proceeds to step **215**. In step **215**, the mobile device attempts to reconnect the data session. The process is similar to step **214** with minor differences.

[0044] In step **216**, a determination is made as to whether the network authentication has failed, i.e. a packet data service authentication rejection is received. In a SIP network, the mobile device is authenticated by the network using CHAP or PAP, which assume that the User Id and Password of the device are known by the network. If the device turns out to be an unknown entity to the network from a packet data services viewpoint, the authentication will fail and packet data services will be refused. If authentication fails, the method proceeds to step **218** where the mobile device enters, or adds, the SID of the system to current blacklist, starts a timer and stops trying to setup a data session on the system until the timer expires. The timer value can be an age timer. Following this step, the method proceeds to step **212** in **Fig. 6A**, where the device allows voice and SMS and informs the user that packet data services are not provided by the network.

[0045] When the device moves to another system, it first checks whether the new system supports packet data services or not. If it does, the device then checks whether the system is in its current blacklist, as outlined in the steps above. If yes, it refrains from making any data call attempts on that system. Otherwise, the device will try to reconnect to keep the data session alive. If it fails authentication, the new system will also be blacklisted and no data retry attempts will take place until the associated age timer expires.

[0046] If, in step **216**, the network successfully authenticates the mobile device, it is determined that the network provides data services to the mobile device and the method proceeds to step **220**. The method also preferably includes within step **218** a step of marking the SID as "not reported". Then, in step **220**, it is determined whether any entry in the current blacklist has not been reported. The term "reporting" here is used to represent any communication of such an entry to a device other than the mobile device, such as a home server associated with the mobile device.

[0047] Therefore, if there is a non-reported entry in the current blacklist, in step **222** the home server is notified of the SID change and any "new" blacklisted SIDs are reported. If there are no non-reported entries in the current blacklist, a preferred step **224** determines whether the current SID is stored in a "once blacklisted" table. The "once blacklisted" table is similar to the current blacklist in structure, as will be outlined below,

except that it keeps a historical list of all SIDs that have been blacklisted within a particular time period. If the current SID is in the "once blacklisted" table, the method proceeds to notify the home server of a change in status of the current SID and it is removed from the "once blacklisted" list. If not, the method proceeds to step **228**, where the mobile device has successfully established or re-established a packet data session and enters a dormant state whenever it is done sending or receiving data.

[0048] In an alternative embodiment, the method further includes a step of "pushing" a current blacklist from a home server to a mobile device. This can easily be accomplished since the home server can be kept up-to-date with respect to data roaming agreements for a given wireless service provider and all the mobile devices that have subscribed to its wireless service can be informed accordingly. In some cases, this blacklist can be a composite current blacklist formed at the home server based on the reports from the mobile devices that belong to the same carrier. If the information is pushed to the mobile device, then it provides advance warning to a mobile device entering a new system. When an mobile device powers up in a RN and registers with the server, the server can also forward the information of currently blacklisted systems so that the mobile device can avoid data originations in such RNs.

[0049] **Fig. 7** illustrates a representation of an exemplary current blacklist according to an embodiment of the present invention. The current blacklist **122** includes information relating to SIDs that are currently listed as the wireless networks where packet data services are not provided. The current blacklist can be stored as a table, with each entry, or row, preferably including the following data: identification of SID **132**; a timer value **134**, such as an age timer; and a flag **136**. The SID identification can include an identification of the corresponding NID. The associated timer starts when the SID is first blacklisted and counts down until its expiry, at which time the entry is preferably removed from the current blacklist. The flag **136** indicates whether the blacklisted SID has been passed to a server, such as a home server, with allowed values preferably being YES and NO. An appropriate initial timer value can be selected, after which the SID will be removed from the blacklist, for example, one month. When a system with a formerly blacklisted SID is next encountered, the availability of packet data services is rechecked. In an alternative embodiment, the entire current blacklist can be reset or cleared when radio services on a mobile device are turned off.

[0050] There are two types of reset conditions under which a current blacklist, or a portion thereof, is cleared: a timer reset condition and a provisioning reset condition. The term "timer reset condition" is used to refer to any instance (such as expiry of an age timer, powering off of the mobile device or its radio) where an individual entry in the current blacklist is to be cleared. For example, a wireless network's entry in the current blacklist is cleared upon expiry of its age timer. After that point, the next time the mobile device encounters that wireless network, it attempts anew to acquire packet data services on the system, in case the situation has changed. A mobile device's current blacklist can alternatively be cleared when the mobile device is turned off, or when the device's radio is turned off.

[0051] The mobile device can also clear the entire current blacklist in response to a provisioning reset condition. A "provisioning reset condition" includes any change in provisioning or authentication parameters, such as user ID or password in SIP. Such a change occurs after a mobile device is provisioned for the first time, or re-provisioned with new parameters. The provisioning process can take place over the air or manually. In the case of the occurrence of a provisioning reset condition, the mobile device automatically clears the current blacklist as it may no longer be valid in light of the changed parameters.

[0052] Whenever the device re-establishes a data session after being refused service on one or more other wireless networks, it can send the list of blacklisted SIDs that has not yet been reported to the home server. In addition, the device also maintains a list of SIDs that were once blacklisted, but now provide packet data services. Once the device notifies the server of status change, the corresponding entries are cleared. When the server is notified of the status change of a wireless network and that the wireless network now provides packet data services, it can also notify other mobile devices of this status change so that all the other mobile devices can clear the entry of that wireless network and will not avoid data originations in that wireless network.

[0053] **Fig. 8** illustrates the relationship between a conventional OSI network layer model **138** and a similar layer model **140** for a typical mobile device. A device driver layer **142**, an operating system layer **144** and a radio layer **146** can collectively be referred to as a radio section. The Java/Radio Interface **148** facilitates communication between the layers in the radio section and those in the Java section. Although the applications in this example are shown as Java-based, they can be based on any other high level language.

The Java section includes a Java Virtual Machine layer **150** and a Java Applications layer **152**. The steps shown in **Fig. 6** are preferably performed at the layers identified as the radio section, although they may alternatively be performed at the layers identified as a Java section.

[0054] The above-described embodiments of the present invention are intended to be examples only. Alterations, modifications and variations may be effected to the particular embodiments by those of skill in the art without departing from the scope of the invention, which is defined solely by the claims appended hereto.

What is claimed is:

1. A mobile device capable of supporting packet data services offered by wireless networks, the mobile device comprising:

a transceiver for exchanging packet data service authentication information with the wireless networks;

a memory;

a current blacklist provided in the memory, the current blacklist identifying wireless networks that do not provide packet data services to the mobile device, the current blacklist being based on previous packet data service authentication rejections; and

a processor for updating the current blacklist in response to newly received packet data service authentication information.

2. The mobile device of claim 1 wherein the current blacklist includes an element selected from the group consisting of: a system identifier and network identifier for each wireless network not providing packet data services to the mobile device; a timer value for each wireless network not providing packet data services to the mobile device; an age timer for each wireless network not providing packet data services to the mobile device; and a flag indicating whether an identification of a blacklisted wireless network has been passed to a server.

3. The mobile device of claim 1 wherein the current blacklist includes a composite current blacklist received from a server.

4. A method of data service discovery for a mobile device having a current blacklist comprising:

detecting a wireless network;

examining the current blacklist stored on the mobile device;

if the detected wireless network is listed in the current blacklist, refraining from making any packet data call attempts for a predetermined period of time; and

otherwise, determining whether the wireless network provides packet data services to the mobile device, and adding the wireless network to the current blacklist if the

wireless network does not provide packet data services to the mobile device.

5. The method of claim 4 further comprising, prior to the step of checking, the step of determining whether the wireless network supports data service.

6. The method of claim 4 wherein the step of determining whether the wireless network provides packet data services to the mobile device comprises the step of authenticating the mobile device on the wireless network.

7. The method of claim 4 further comprising a step selected from the group consisting of: starting an age timer associated with a wireless network that is added to the current blacklist; clearing an age timer associated with a wireless network in response to satisfaction of a reset condition; notifying a server of a newly blacklisted wireless network; and receiving a composite current blacklist from a server.

8. The method of claim 4 further comprising the step of clearing the current blacklist in response to a provisioning reset condition.

9. The method of claim 4 further comprising a step selected from the group consisting of: sending a notification to the server if a mobile device finds a wireless network which was not previously providing packet data services to the mobile device and is now providing packet data services to the mobile device; and sending a notification from the server to other mobile devices to clear the entry of a wireless network which was previously not providing packet data services but currently is providing packet data services.

10. A method of packet data service notification in a wireless network, the wireless network including a server and a mobile device, the method comprising:

receiving at the server a registration of a newly powered-up mobile device;

retrieving a server-stored current blacklist identifying wireless networks that do not provide packet data services to the newly powered-up mobile device; and

sending the server-stored current blacklist from the server to the newly powered-up mobile device for reception by and storage on the mobile device.

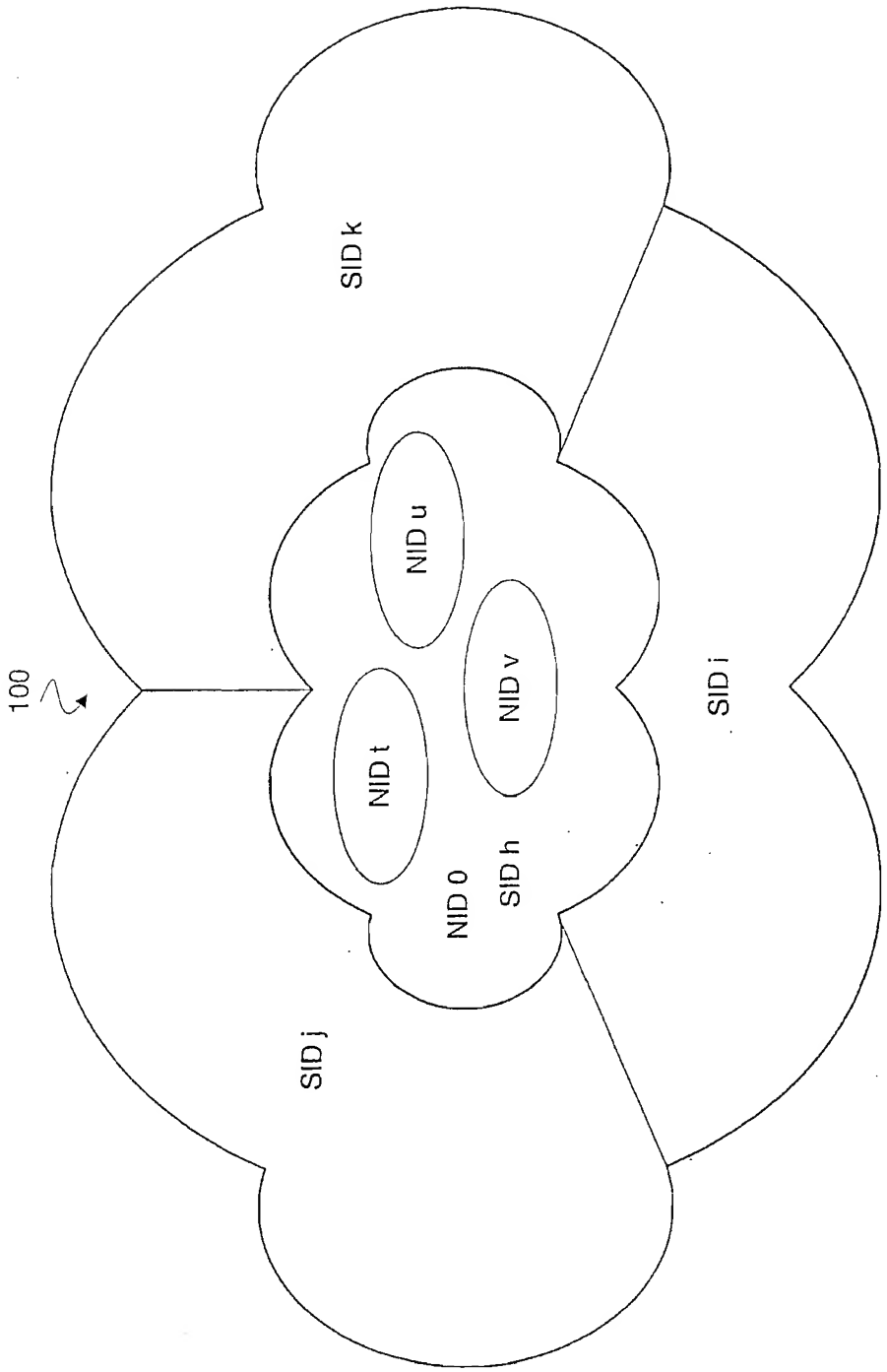


FIG. 1
PRIOR ART

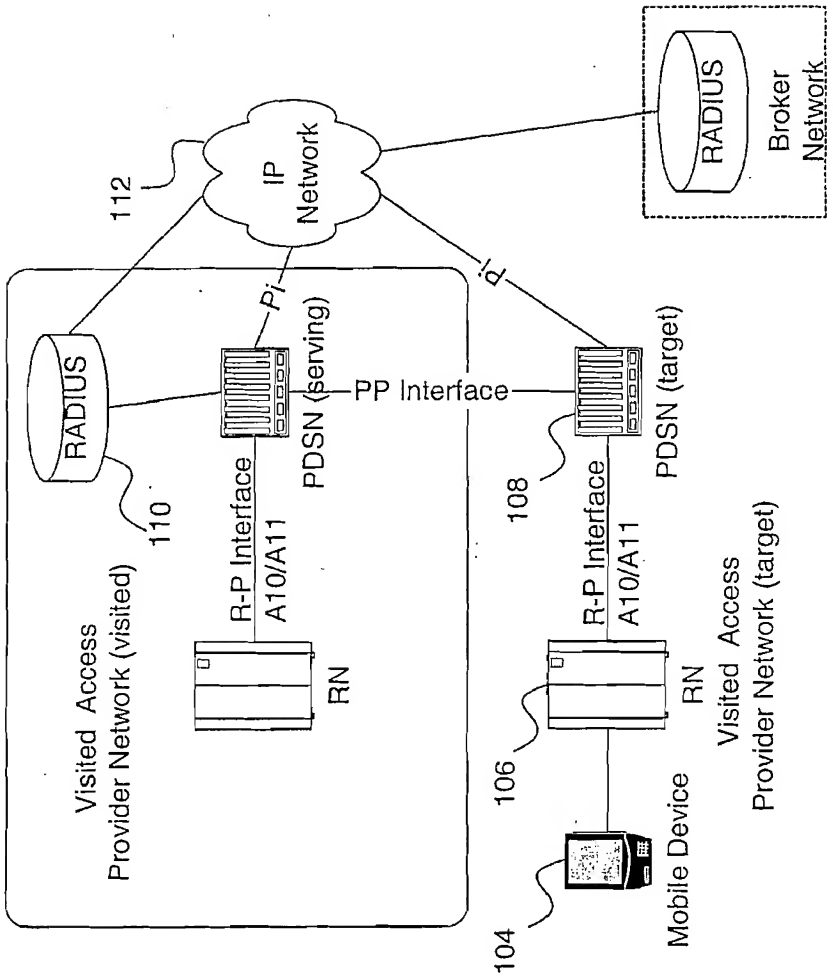


FIG. 3
PRIOR ART

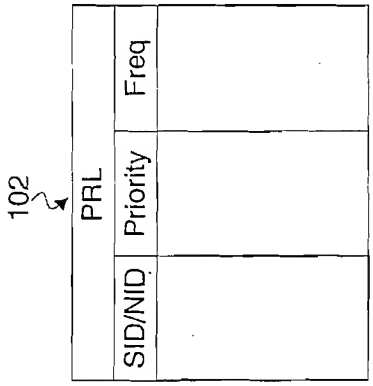


FIG. 2
PRIOR ART

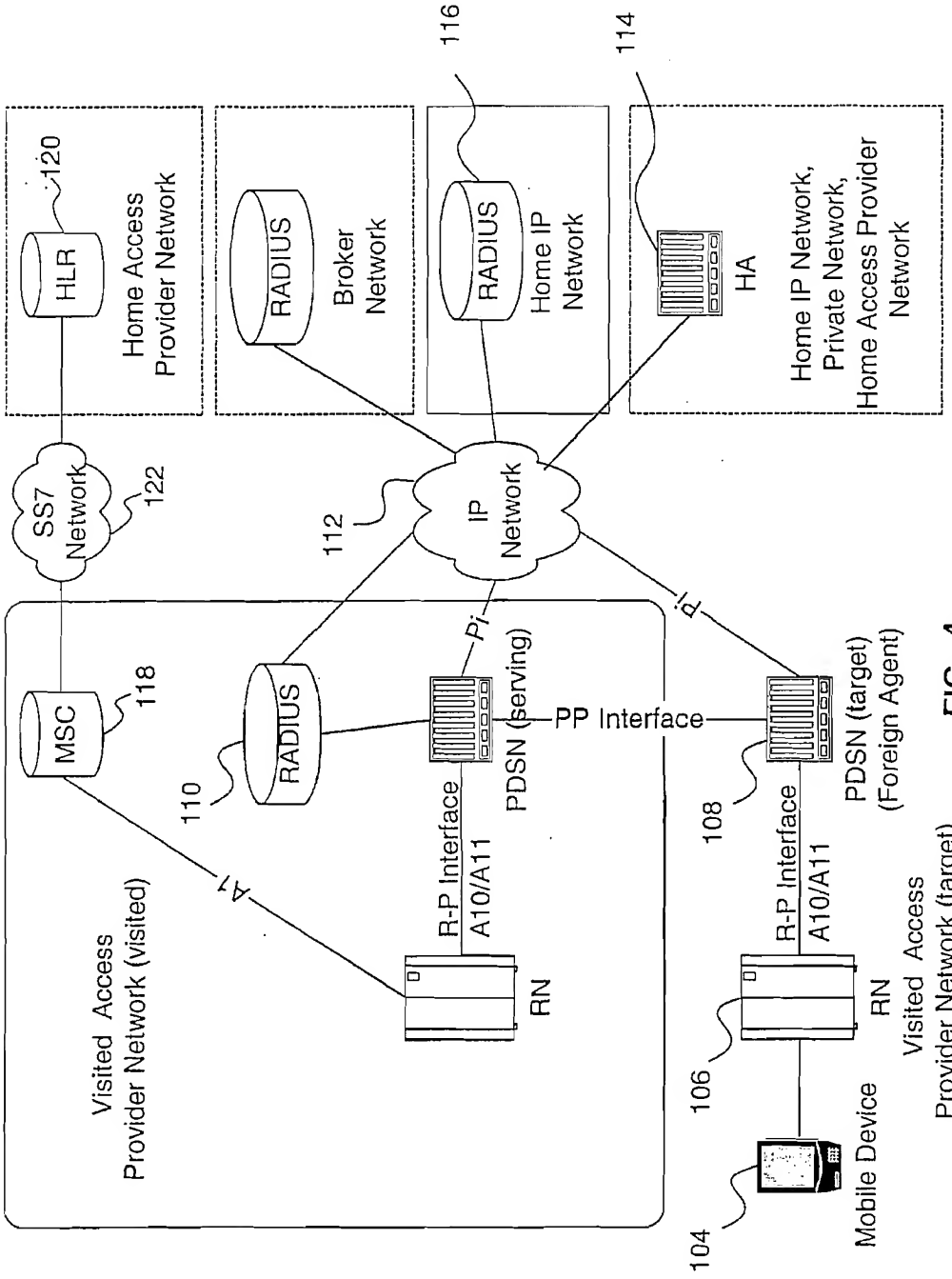


FIG. 4
PRIOR ART

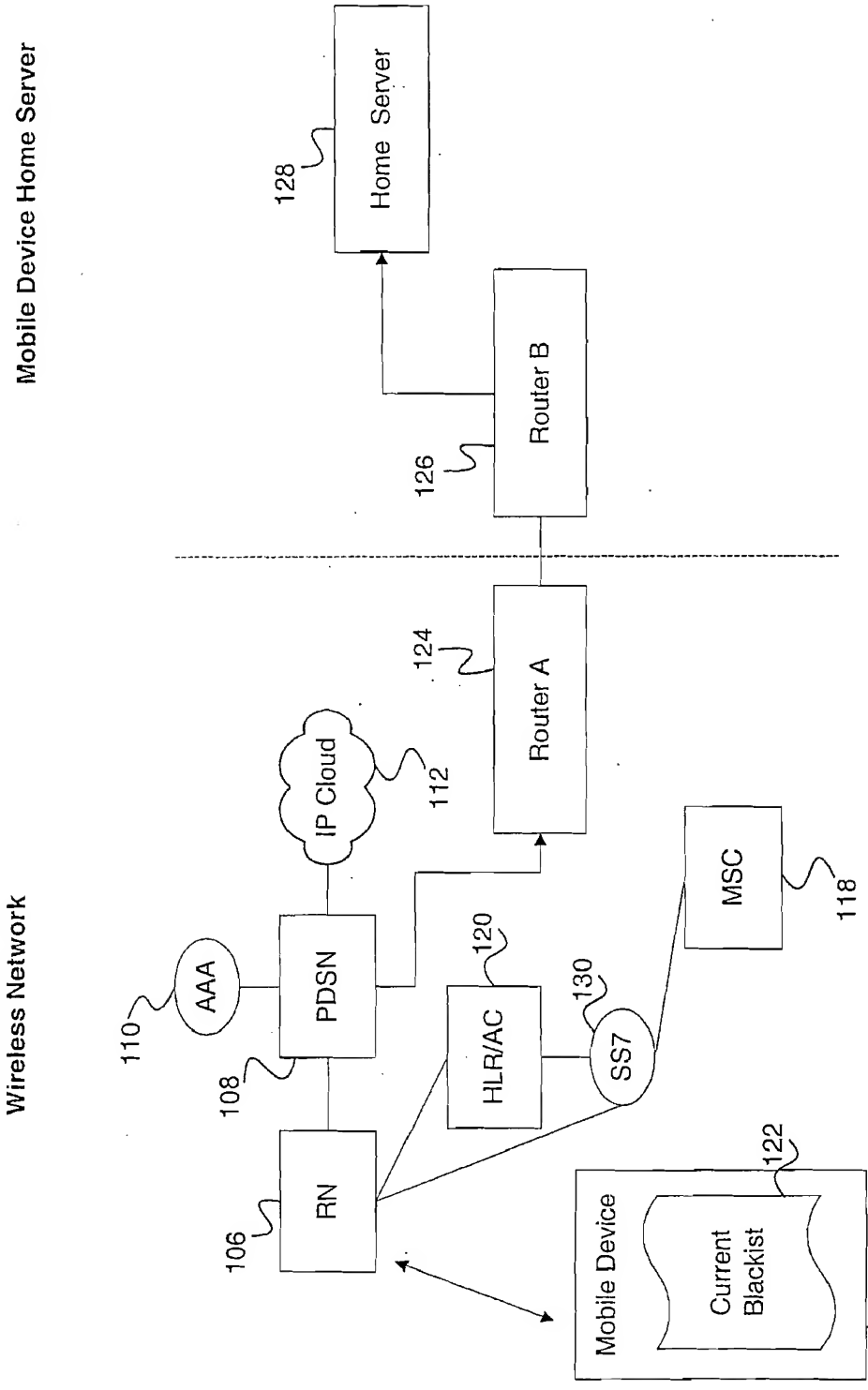
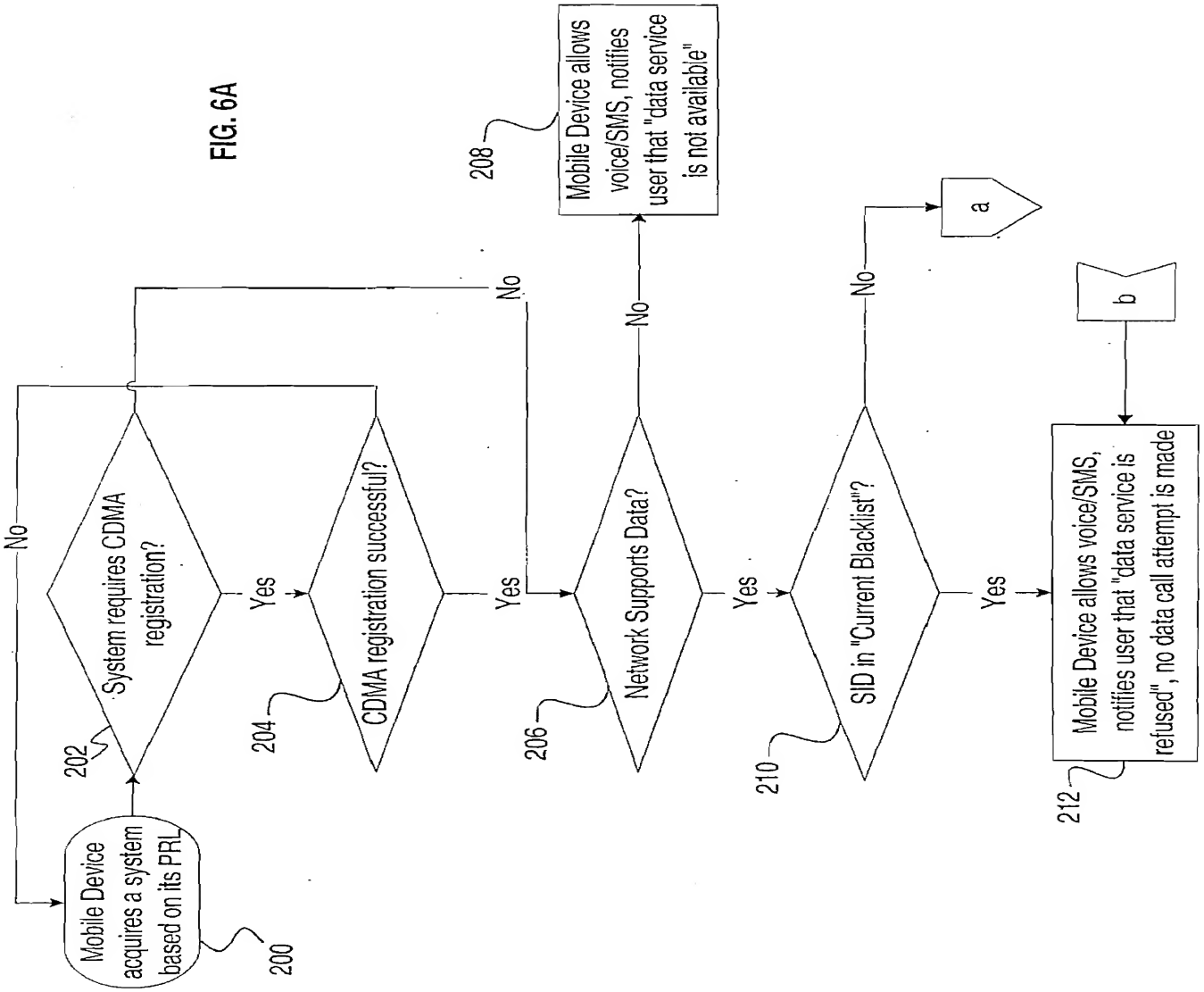

Mobile Device Home Server
Wireless Network
128
Home Server
126
Router B
124
Router A
112
IP Cloud
110
AAA
108
PDSN
106
RN
120
HLR/AC
130
SS7
MSC
118
122
Current Blackist
Mobile Device
104

FIG. 5

FIG. 6A


Mobile Device acquires a system based on its PRL
200
System requires CDMA registration?
202
No
Yes
CDMA registration successful?
204
No
Yes
Network Supports Data?
206
No
Yes
Mobile Device allows voice/SMS, notifies user that "data service is not available"
208
SID in "Current Blacklist"?
210
No
Yes
a
b
Mobile Device allows voice/SMS, notifies user that "data service is refused", no data call attempt is made
212

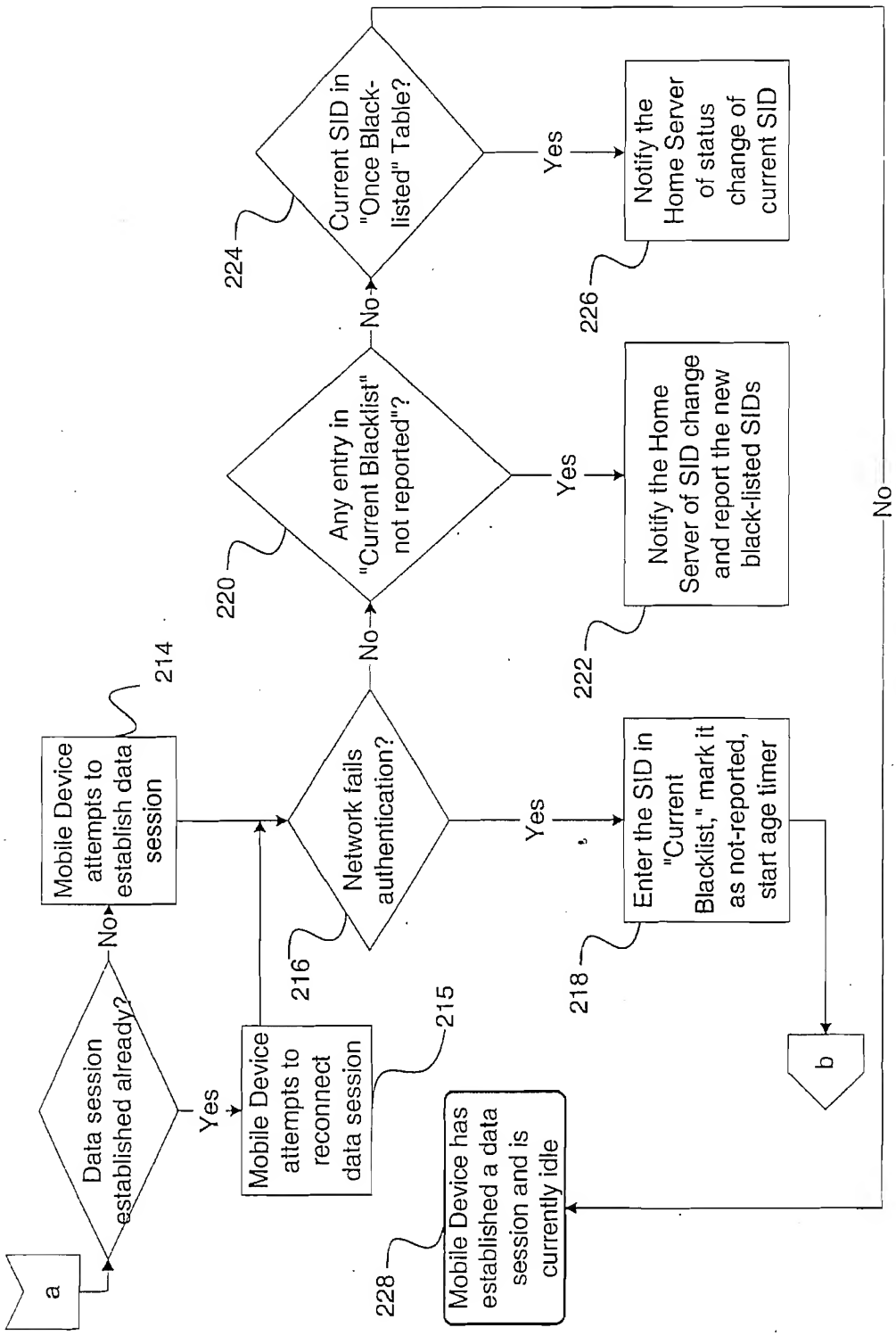

a
Data session established already?
No
Yes
Mobile Device attempts to establish data session
214
Mobile Device attempts to reconnect data session
215
Network fails authentication?
216
Yes
No
Enter the SID in "Current Blacklist," mark it as not-reported, start age timer
218
b
Any entry in "Current Blacklist" not reported"?
220
Yes
No
Notify the Home Server of SID change and report the new black-listed SIDs
222
Current SID in "Once Black-listed" Table?
224
Yes
No
Notify the Home Server of status change of current SID
226
Mobile Device has established a data session and is currently idle
228

FIG. 6B

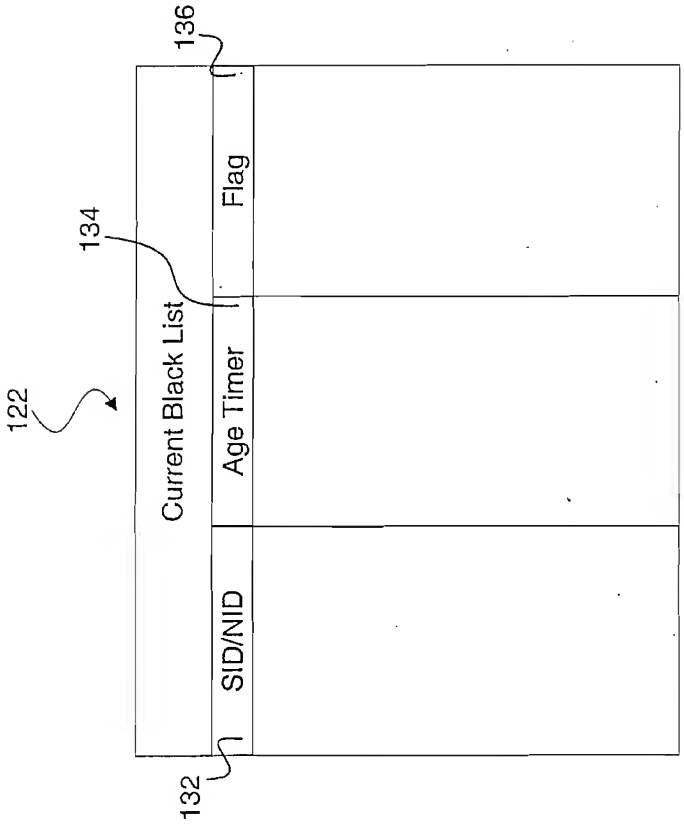


FIG. 7

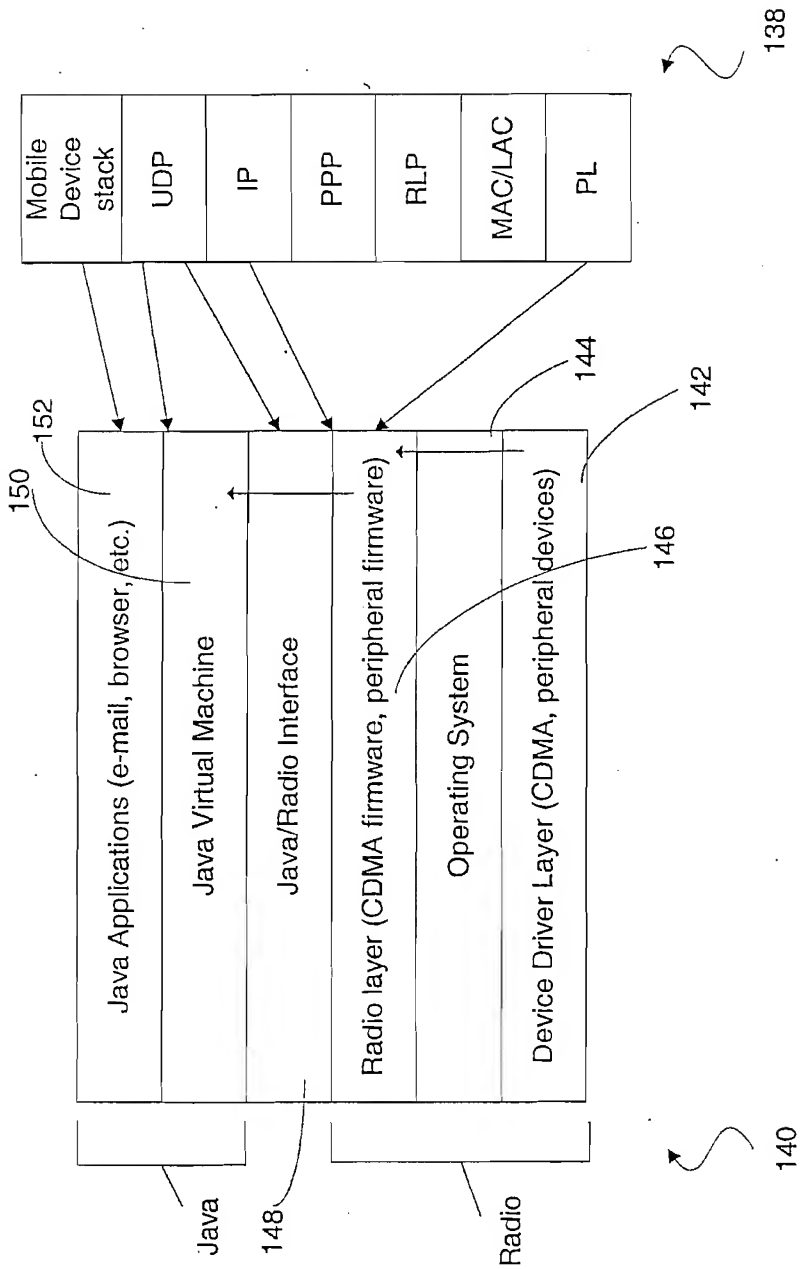

Mobile Device stack
UDP
IP
PPP
RLP
MAC/LAC
PL
138
152
150
144
142
146
Java Applications (e-mail, browser, etc.)
Java Virtual Machine
Java/Radio Interface
Radio layer (CDMA firmware, peripheral firmware)
Operating System
Device Driver Layer (CDMA, peripheral devices)
140
Java
148
Radio

FIG. 8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 03/00955

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04Q7/38 H04Q7/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2002/123348 A1 (WILLARS PAR ET AL) 5 September 2002 (2002-09-05) paragraphs '0034!,'0050!,'0055!,'0087!,'0093!,'0094!, '0102!-'0109!; figure 3	1,5,6,9 2-4,7,8, 10
Y	US 2002/147012 A1 (YAU KWOK WING ET AL) 10 October 2002 (2002-10-10) paragraphs '0003!,'0009!,'0010!,'0019!-'0025!,'0027!, '0037!,'0040!,'0045!-'0057!,'0061!,'0064!	3,10

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 September 2003	05/12/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Mele, M

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 03/00955

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 01 05169 A (NOKIA MOBILE PHONES LTD ;NOKIA INC (US)) 18 January 2001 (2001-01-18) page 2, line 35 -page 3, line 1 page 3, line 9-12 page 4, line 31 -page 5, line 1 page 5, line 28 -page 6, line 5 page 6, line 35 -page 7, line 19 page 8, line 1 - line 20 page 9, line 29 -page 10, line 33 page 11, line 38 -page 12, line 12 page 13, line 34 -page 14, line 5 ---	2,4,7,8
A	WO 01 54435 A (TELECOMM SYSTEMS INC) 26 July 2001 (2001-07-26) page 5, line 25 -page 6, line 15 ---	1-10
A	GB 2 315 193 A (ORANGE PERSONAL COMM SERV LTD) 21 January 1998 (1998-01-21) page 12, line 5-20 page 13, line 9-15 page 14, line 23 -page 15, line 17 page 17, line 5 - line 23 page 19, line 11 - line 19 ---	1-10
A	"DIGITAL CELLULAR TELECOMMUNICATIONS SYSTEM (PHASE 2+);SPECIFICATION OF THE SUBSCRIBER IDENTITY MODULE - MOBILE EQUIPMENT (SIM - ME) INTERFACE (GSM 11.11 VERSION 5.9.1)" ETS 300 977, XX, XX, October 1998 (1998-10), pages 1-127, XP000863809 page 64 -page 65 -----	1-10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 03/00955

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002123348 A1	05-09-2002	AU 761957 B2	12-06-2003
		AU 3992600 A	23-10-2000
		BR 0009553 A	08-01-2002
		CA 2368468 A1	12-10-2000
		CN 1354963 T	19-06-2002
		EP 1166586 A1	02-01-2002
		JP 2002541747 T	03-12-2002
		WO 0060895 A1	12-10-2000
		TW 477132 B	21-02-2002
		ZA 200107954 A	27-09-2002
		WO 02065789 A2	22-08-2002
		WO 02065805 A1	22-08-2002
		WO 02065806 A1	22-08-2002
		WO 02065807 A1	22-08-2002
		WO 02065808 A1	22-08-2002
		US 2002111180 A1	15-08-2002
		US 2003013443 A1	16-01-2003
		US 2002151304 A1	17-10-2002
US 2002147012 A1	10-10-2002	GB 2369265 A	22-05-2002
		AU 9217201 A	22-03-2002
		CN 1381150 T	20-11-2002
		EP 1228656 A2	07-08-2002
		WO 0221861 A2	14-03-2002
		TW 498670 B	11-08-2002
WO 0105169 A	18-01-2001	AU 7386100 A	30-01-2001
		EP 1195069 A2	10-04-2002
		WO 0105169 A2	18-01-2001
WO 0154435 A	26-07-2001	US 6564055 B1	13-05-2003
		AU 3285601 A	31-07-2001
		WO 0154435 A1	26-07-2001
GB 2315193 A	21-01-1998	AU 728172 B2	04-01-2001
		AU 1608997 A	02-02-1998
		EP 0910924 A2	28-04-1999
		WO 9802008 A2	15-01-1998
		JP 2000514267 T	24-10-2000
		ZA 9705864 A	25-01-1999